特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　０２０６３８ＰＣＴ	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０３／１２０２２	国際出願日 （日.月.年）　１９．０９．２００３	優先日 （日.月.年）　２０．０９．２００２
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８		
出願人（氏名又は名称） パイオニア株式会社		

１．この報告書は、ＰＣＴ３５条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で　5　ページからなる。

３．この報告には次の附属物件も添付されている。

a [×] 附属書類は全部で　3　ページである。

[×] 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第６０７号参照）

[ ] 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b [ ] 電子媒体は全部で＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。（実施細則第８０２号参照）

４．この国際予備審査報告は、次の内容を含む。

[×] 第Ｉ欄　国際予備審査報告の基礎
[ ] 第Ⅱ欄　優先権
[×] 第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
[ ] 第Ⅳ欄　発明の単一性の欠如
[×] 第Ⅴ欄　ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
[ ] 第Ⅵ欄　ある種の引用文献
[ ] 第Ⅶ欄　国際出願の不備
[×] 第Ⅷ欄　国際出願に対する意見

国際予備審査の請求書を受理した日 ２０．０４．２００４	国際予備審査報告を作成した日 ２１．０１．２００５
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　5M　9364 中里 裕正 電話番号　０３－３５８１－１１０１　内線　３５９９

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００４年１月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１２０２２

第Ｉ欄　報告の基礎

１．この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、＿＿＿＿＿＿ 語による翻訳文を基礎とした。
それは、次の目的で提出された翻訳文の言語である。
☐ ＰＣＴ規則12.3及び23.1(b)にいう国際調査
☐ ＰＣＴ規則12.4にいう国際公開
☐ ＰＣＴ規則55.2又は55.3にいう国際予備審査

２．この報告は下記の出願書類を基礎とした。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☒ 明細書
第 1-32 ページ、 出願時に提出されたもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 請求の範囲
第 ＿＿＿＿ 項、 出願時に提出されたもの
第 ＿＿＿＿ 項*、 ＰＣＴ１９条の規定に基づき補正されたもの
第 1-7 項*、 19.10.2004 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ 項*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 図面
第 1-18 ページ/~~図~~、 出願時に提出されたもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

３．☒ 補正により、下記の書類が削除された。

☐ 明細書　第 ＿＿＿＿ ページ
☒ 請求の範囲　第 8,9 項
☐ 図面　第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること） ＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること） ＿＿＿＿

４．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

☐ 明細書　第 ＿＿＿＿ ページ
☐ 請求の範囲　第 ＿＿＿＿ 項
☐ 図面　第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること） ＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること） ＿＿＿＿

＊４．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１２０２２

第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての見解の不作成

1．次に関して、当該請求の範囲に記載されている発明の新規性、進歩性又は産業上の利用可能性につき、次の理由により審査しない。

☐ 国際出願全体

☒ 請求の範囲 7

理由：

☒ この国際出願又は請求の範囲 7 は、国際予備審査をすることを要しない次の事項を内容としている（具体的に記載すること）。

情報が特定のシステムにより生成されたということは、情報を記録する記録媒体とは何ら関係のないことであるから、かかる情報を記録した記録媒体は、情報を単に提示するものにすぎない。

なお出願人は答弁書において、鍵情報は記録媒体に記録された情報の再生を制御する機能を有している旨を主張しているが、鍵情報それ自体に機器を制御する機能が備わっているはずもないから、かかる主張はその根拠を欠くものである。

☐ 明細書、請求の範囲若しくは図面（次に示す部分）又は請求の範囲 の記載が、不明確であるため、見解を示すことができない（具体的に記載すること）。

☐ 全部の請求の範囲又は請求の範囲 が、明細書による十分な裏付けを欠くため、見解を示すことができない。

☐ 請求の範囲 について、国際調査報告が作成されていない。

☐ ヌクレオチド又はアミノ酸の配列表が、実施細則の附属書Ｃ（塩基配列又はアミノ酸配列を含む明細書等の作成のためのガイドライン）に定める基準を、次の点で満たしていない。

書面による配列表が
☐ 提出されていない。
☐ 所定の基準を満たしていない。

コンピュータ読み取り可能な形式による配列表が
☐ 提出されていない。
☐ 所定の基準を満たしていない。

☐ コンピュータ読み取り可能な形式によるヌクレオチド又はアミノ酸の配列表に関連するテーブルが、実施細則の附属書Ｃの２に定める技術的な要件を、次の点で満たしていない。

☐ 提出されていない。
☐ 所定の技術的な要件を満たしていない。

☐ 詳細については補充欄を参照すること。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１２０２２

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（N）	請求の範囲		有
	請求の範囲	1-6	無
進歩性（ＩＳ）	請求の範囲		有
	請求の範囲	1-6	無
産業上の利用可能性（ＩＡ）	請求の範囲	1-6	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：The LSD Broadcast Encryption Scheme,
Lecture Notes in Computer Science, Vol.2442, p.47-60, 2002.09.09(JICST受入日)
2.2 The Basic LSD Scheme, 2.3 The General LSD Scheme

請求の範囲１－６は、国際予備審査において新たに引用された文献１により新規性を有しない。文献１には、階層に分割した木構造に基づいた差分集合に鍵情報を割り当てることが記載されている。差分集合は階層毎に生成されるものであるから、かかる差分集合は階層毎に独立して生成されるものであるといえる。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１２０２２

第Ⅷ欄　国際出願に対する意見

請求の範囲、明細書及び図面の明瞭性又は請求の範囲の明細書による十分な裏付についての意見を次に示す。

請求の範囲１，５には「先祖ノード以下の階層に存在し、子孫ノード以下の階層には存在しない当該部分木のリーフ又は当該部分木のリーフの下位に存在する前記木構造のリーフに割り当てられた受信者の差分集合」なるものが記載されている。しかしながら、これらの記載における「階層」に存在する、あるいは存在しない部分木のリーフとは、如何なるものであるのかということが不明である。また、そのようなリーフに割り当てられた受信者の「差分集合」とは、如何なるものであるのかという点も不明である。

請 求 の 範 囲

1．（補正後） 複数の情報受信者をリーフに割り当てた木構造を規定する手段と、

前記木構造を、所定数の階層からなるマクロレイヤ毎に分割して複数の部分木を規定する手段と、

前記部分木内に存在する先祖ノードと子孫ノードにより定義される差分集合であって、前記先祖ノード以下の階層に存在し、かつ、前記子孫ノード以下の階層には存在しない当該部分木のリーフ又は当該部分木のリーフの下位に存在する前記木構造のリーフに割り当てられた情報受信者の差分集合を、前記部分木毎に独立に定義する手段と、

前記差分集合の各々に１つの暗号／復号鍵を割り当てる手段と、

前記複数の情報受信者の各々に対して、当該情報受信者が属する全ての差分集合に割り当てられた暗号／復号鍵を割り当てる手段と、を有することを特徴とする鍵管理システム。

2．（補正後） 前記木構造のリーフに割り当てられた複数の情報受信者のうち、特定の情報受信者のみが復号可能な鍵情報を生成する鍵情報生成手段をさらに備えることを特徴とする請求の範囲第１項に記載の鍵管理システム。

3．（補正後） 前記複数の情報受信者のうちの特定の情報受信者について、当該情報受信者を含む全ての前記差分集合に割り当てられた暗号／復号鍵を求めることを可能とする秘密情報を当該情報受信者に割り当てる手段をさらに備えることを特徴とする請求の範囲第１項に記載の鍵管理システム。

4．（補正後） 前記木構造のリーフに割り当てられた複数の情報受信者のうち、特定の情報受信者のみが復号可能な鍵情報を生成する鍵情報生成手段と、

前記特定の情報受信者について、当該情報受信者を含む全ての前記差分集合に割り当てられた暗号／復号鍵を求めることを可能とする秘密情報を当該情報受信

者に割り当てる手段と、

前記鍵情報及び前記秘密情報を用いて、前記特定の情報受信者を含む全ての前記差分集合に割り当てられた暗号／復号鍵を求める手段と、を備えることを特徴とする請求の範囲第１項に記載の鍵管理システム。

５．（補正後） 複数の情報受信者をリーフに割り当てた木構造を規定する工程と、

前記木構造を、所定数の階層からなるマクロレイヤ毎に分割して複数の部分木を規定する工程と、

前記部分木内に存在する先祖ノードと子孫ノードにより定義される差分集合であって、前記先祖ノード以下の階層に存在し、かつ、前記子孫ノード以下の階層には存在しない当該部分木のリーフ又は当該部分木のリーフの下位に存在する前記木構造のリーフに割り当てられた情報受信者の差分集合を、前記部分木毎に独立に定義する工程と、

前記差分集合の各々に１つの暗号／復号鍵を割り当てる工程と、

前記複数の情報受信者の各々に対して、当該情報受信者が属する全ての差分集合に割り当てられた暗号／復号鍵を割り当てる工程と、を有することを特徴とする鍵管理方法。

６．（補正後） コンピュータを備える装置において実行される鍵管理プログラムであって、

複数の情報受信者をリーフに割り当てた木構造を規定する手段、

前記木構造を、所定数の階層からなるマクロレイヤ毎に分割して複数の部分木を規定する手段、

前記部分木内に存在する先祖ノードと子孫ノードにより定義される差分集合であって、前記先祖ノード以下の階層に存在し、かつ、前記子孫ノード以下の階層には存在しない当該部分木のリーフ又は当該部分木のリーフの下位に存在する前記木構造のリーフに割り当てられた情報受信者の差分集合を、前記部分木毎に独立に定義する手段、

前記差分集合の各々に１つの暗号／復号鍵を割り当てる手段、

前記複数の情報受信者の各々に対して、当該情報受信者が属する全ての差分集合に割り当てられた暗号／復号鍵を割り当てる手段、として前記コンピュータを機能させることを特徴とする鍵管理プログラム。

7．（補正後） 請求の範囲第２項に記載の鍵管理システムより生成された鍵情報を記録した記録媒体。

8．（削除）

9．（削除）